A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems

Dimitrios Sikeridis*, Ali Bidram*, Michael Devetsikiotis*, and Matthew J. Reno¶
*Department of Electrical and Computer Engineering, The University of New Mexico, Albuquerque, NM, USA
¶Sandia National Laboratories, Albuquerque, NM, USA
{dsike, bidram, mdevets}@unm.edu, mjreno@sandia.gov

Abstract—**Distribution and transmission protection systems are considered vital parts of modern smart grid ecosystems due to their ability to isolate faulted segments and preserve the operation of critical loads. Current protection schemes increasingly utilize cognitive methods to proactively modify their actions according to extreme power system changes. However, the effectiveness and robustness of these information-driven solutions rely entirely on the integrity, authenticity, and confidentiality of the data and control signals exchanged on the underlying relay communication networks. In this paper, we outline a scalable adaptive protection platform for distribution systems, and introduce a novel blockchain-based distributed network architecture to enhance data exchange security among the smart grid protection relays. The proposed mechanism utilizes a tiered blockchain architecture to counter the current technology limitations providing low latency with better scalability. The decentralized nature removes singular points of failure or contamination, enabling direct secure communication between smart grid relays. We also present a security analysis that demonstrates how the proposed framework prohibits any alterations on the blockchain ledger providing integrity and authenticity of the exchanged data (e.g., real-time measurements/relay settings). Finally, the performance of the proposed approach is evaluated through simulation on a blockchain benchmarking framework with the results demonstrating a promising solution for secure smart grid protection system communication.**

Index Terms—**Smart Grid, Cyber-Physical Security, Adaptive Protection Systems, Blockchain Technology**

I. Introduction

Power system protection is a key grid component responsible for detecting and clearing faults on different equipment, e.g., generators, lines, and transformers [1]. Its key elements are protection relays which are responsible for fault detection and isolation on their protected equipment. A protection system is expected to ascertain requirements for sensitivity (i.e., the ability of timely detecting and isolating faulted regions to avoid damaging other equipment), and selectivity (i.e., the intelligent isolation of faults to minimize the number of customers experiencing power outage). The 2003 Northeast blackout, the world's second most widespread blackout, highlights how a well-coordinated protection system could have prevented the spread of cascading power outages [2]. Also, the 2018 assessment of North American Electric Reliability Corporation reports that 9% of the total grid interruptions in the last five years are related to relay misoperations [3].

The design of protection systems includes physical components coupled with communication-enabled intelligence to implement the protection logic resulting in large scale cyber-physical formations. Due to the infrastructure's critical role, security is paramount especially since the rapid automation of the grid leads to completely digital protection components with increased capabilities in terms of computing power, embedded storage, and communications. This shift to smart industrial devices, introduces vulnerabilities pertaining to the cyber fabric of the installations that can in turn affect physical components, which is an important national security threat in case critical loads are targeted [4], [5].

A. Related Work

Conventional protection systems utilize fixed settings for protective relays which are well-tuned only for the normal operating conditions [6], and do not account for extreme events, e.g., hurricanes, where the system is prone to multiple simultaneous faults and line outages, and the power system undergoes drastic topology changes. Moreover, the coordination of the conventional protection system can be affected by the large number of distributed energy resources (DER) due to their different fault current levels and potential for reverse power flow [7]. To tackle these challenges, adaptive protection schemes have been proposed to modify the protective actions according to system condition changes, as in [8], where authors utilize numerical directional overcurrent relays coupled with commercial mathematical programming tools and optimization solvers.

Focusing on the cyber layer, power systems automation infrastructure often utilizes centralized communication network with a central substation controller for monitoring data and sending control/protection signals [9]. Such centralized data aggregation creates security challenges as parts of the infrastructure are in risk of being paralyzed in case of an attack on the control center (e.g. 2016 attack against Ukraine's substation [5]). In addition, the emerging digital nature of protection components makes them vulnerable to a series of modern security threats including false data injection attacks [10], grid command tampering (e.g., in Puerto Rico [5]), Aurora attacks, and privacy leaks [5].

Recently, towards enhancing the security of power systems infrastructure, the emerging Blockchain technology [11] has been utilized to achieve build-in privacy, integrity, authenticity, and confidentiality of the exchanged data and control signals. In [12], the authors propose a blockchain-based scheme for

978-1-7281-3893-0/20/$31.00 ©2020 IEEE

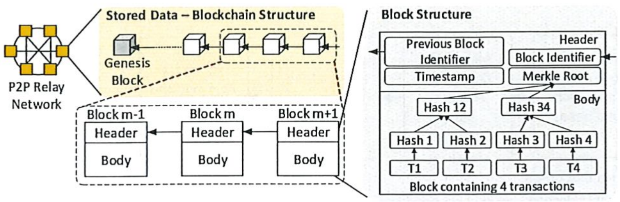

Fig. 2: Blockchain Data Structure

outage of neighboring branches, distribution transformers, and DERs.

4) Setting Calculation Module: This module uses the coordination study results to recommend new settings for the protection devices. Any flagged relay misoperation or CTI violation in the coordination study results is taken into consideration. This module identifies the misoperating protection devices and recommends new settings based on a set of predefined protection rules. These protection rules are electric power utility specific and determine the acceptable protection practices and setting ranges for the protection devices.

III. Blockchain-based APP Network Architecture

A. Blockchain Preliminaries and Considerations

Blockchain relies on a purely distributed and peer-to-peer (P2P) networking topology and can be described as a distributed and transparent public ledger (data structure) replicated and shared among the P2P network entities. Participating nodes, utilize a private public key encryption model to issue transactions (any data exchange) between them. Peer nodes verify the transaction signatures and data before appending them in records termed "blocks" that have specific capacity and consist of a header and a body. The block's body stores the data transactions while the blockchain maintains blocks chronological order by cryptographically chaining them to their predecessors through the header. The blockchain's first block is known as "genesis" block. Each block's header contains its identifier, that is derived through a cryptographic hash of the included transactions, the previous block's identifier, and a publish timestamp. In addition, the header includes a Merkle tree root that is created by hashing the included transactions' IDs in pairs building a hash tree. Fig. 2 shows the structure of a blockchain P2P network's components.

Newly created blocks are permanently added to the blockchain using an established set of rules termed distributed consensus protocol that ensures the agreement among the independent nodes of a common global blockchain-data state (transaction content, and order). A variety of distributed consensus algorithms has been proposed (highly active research topic) with diverse impact on the scalability and performance of Blockchain implementations [16]. At a higher level, depending on the specific application and consensus approach, blockchain systems can be either public (permissionless, e.g., Bitcoin) or private (permissioned). In public blockchains any node can take part in the network, issuing transactions, validating and publishing new blocks while maintaining a full copy of the ledger. They usually accommodate large number of nodes and utilize Proof-of-Work (PoW)-based consensus protocols where a miner node collects transactions into a block and only after successfully solves a computationally hard puzzle can append the block into the chain. The aim is to create an environment tolerant to pseudo identities, and malicious behaviour by making any tampering of block contents extremely costly. To the contrary, in private blockchains each node has to be authenticated and strictly identified. Since they admit tighter control on participants and synchronization, they utilize more conventional Byzantine Fault-Tolerant protocols and voting mechanisms to reach consensus without computationally expensive proofs [16].

Given the above, the incorporation of blockchain architectures into smart grid systems poses challenges. Their design and consensus protocol functionality that provides decentralization, and fault tolerance come at a cost on scalability, and achievable throughput. In addition, blockchain implementations that rely on puzzle solving are power consuming and require nodes with high computational capabilities. Finally, since the distributed ledger continuously grows with new entries, a single blockchain containing all relay nodes would consume more local storage space with poor scaling. Our proposed design aims to mitigate these challenges while considering the specific communication needs of grid protection systems where (a) geographically close or neighboring relays need to exchange measurements or settings, (b) measurements should be periodically reported to the substation, while (c) the latter can convey setting updates to the desired relays.

B. Modular APP Network Design and Operation

For the considered protection system infrastructure, we will utilize a private blockchain logic which provides extra security through strict node authentication, higher transaction throughput, and the ability to utilize a computationally-light consensus mechanism. In addition, while all relay nodes maintain routing functionalities for transaction propagation and verification, our design utilizes nodes of two roles, namely "light-client" and "full-client". Full-client relays maintain a complete and updated replica of the blockchain, are able to issue and verify transactions, and are able to publish new blocks changing the state of the chain. Relays acting as light-client spend less computational resources and retain locally only a copy of each block's header. While they can issue and validate transactions (using the headers' copy), they cannot add new blocks.

In addition, in order to improve the system's scalability and efficiency, we adopt a tiered design where geographically close relays, acting as "full-clients", form separate "sidechains" and select a "Leader" node responsible for adding new blocks to the internal ledger. These sidechains are part of a greater central blockchain, termed "mainchain" that connects them with substation nodes which act as "full-clients" of the mainchain keeping a full record of the data and operating as mining nodes. In order to reduce the storage requirements of the "Leader" nodes, they participate to the mainchain as "light-client" members. The use of sidechains enables relays to retain measurements only from neighbors locally, while avoiding val-

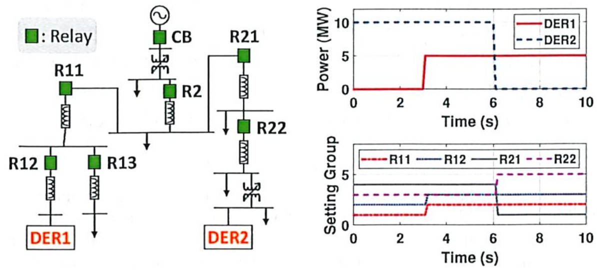

Fig. 4: (a) Simulated Power System and (b) APP Operation

3) Fault Tolerance: The utilized distributed consensus protocol introduces identification of Byzantine failures and achieves agreements between relays despite the possible existence of malicious behaviour of dishonest nodes. Also, all participating relays or substation nodes retain identical replicas of the shared chains. Thus, any node can identify measurement or setting leakages and mitigate them autonomously. Finally, the distributed nature of the ledger and its existence in multiple locations ensures resiliency in case of multiple relay malfunction, and rapid infrastructure recovery which is a crucial attribute of distribution and transmission protection systems.

4) Impact and Consequences: While intercepting protection relay measurements poses relatively minor privacy concerns, the major risks are impacts to the sensitivity (tripping when there is a fault) and selectivity (not tripping when there is not a fault) of the protection system. Modifying data flowing from the relays or settings communicated by the substation could decrease the protection system's dependability. For example, by clearing settings on the relays, fault may go undetected for long periods of time and damage equipment. On the other hand, forcing breakers to operate could cause blackout for sections of the system. It is also important that the APPMS only has access to the required settings in the relays to mitigate risks like malicious firmware updates.

Moreover, the addition and synchronization of new relays into the sidechain is easily facilitated, with each Leader being responsible for the relay's authentication as a legitimate, non-malicious participant. Finally, the underlying secure communication architecture enables the automatic and secure execution of protection system maintenance tasks with relay rekeying being a case in point. This can be a cost efficient alternative to the manual rekeying of thousands relays that includes labor costs and is prone to security holes, while blockchain-based dynamic key management is already considered as a viable solution for cyber-physical systems [17].

V. Performance Evaluation

This section presents a numerical evaluation of the proposed solution in terms of overall communication efficiency. Our simulations consider a distribution circuit whose single line diagram is shown in Fig. 4-a. Each relay is simulated on a separate virtual node within our network hosted by machines with E5-1620 3,6 GHz CPUs, and 16 GB RAM. To closely imitate relay hardware specifications each node is assigned a single processor core with 2 GB RAM, running Ubuntu 18.04.

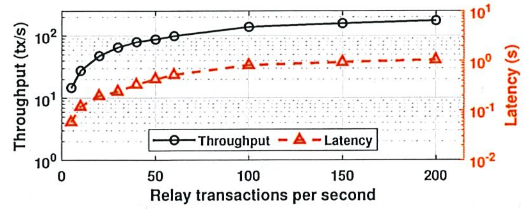

Fig. 5: Performance vs. increasing relay transaction rates

First, we demonstrate the functionality of the adaptive protection system with a sample simulation that focuses on adopting new setting groups for relays after the generation level of DERs are changing drastically. It is assumed that R11, R12, R21, and R22 are microprocessor relays with multiple predefined setting groups selected interchangeably through the adaptive protection system. Fig. 4-b (top) shows the real-time active power measurement of DERs that are sent to APPMS through the blockchain-based communication system. As seen, DER1 and DER2 generation change drastically at $t = 3$ sec and $t = 6$ sec, respectively. These changes are detected by the APPMS, and in response the APA (see Section II) chooses new setting groups for protection relays R11, R12, R21, and R22 to ensure protection system's coordination after the active power changes are satisfied. Impacted relay setting group changes are shown in Fig. 4-b (bottom).

Second, we focus on the communication framework and evaluate its performance in terms of transaction throughput, i.e., the number of transactions successfully included into a block and attached to the ledger per second, and latency, i.e., the elapsed time between a transaction generation and the confirmation reception (response time per transaction). Based on the power system of Fig. 4, our topology consists of two sidechains with four nodes, i.e., {R11, R12, R13, DER1}, and {R2, R21, R22, DER2}. For the blockchain simulation we deployed a modified version of the BLOCKBENCH tool [15], with a Hyperledger Fabric backend. Also, in order to imitate adjustable load generation by the relay clients, we will utilize the YCSB workload [18] which supports different ratios of read/write operations on the blockchain ledger.

In our experiments, the two sidechains operate simultaneously, and consist of three transaction issuers and the Leader. For the performance measurements we monitored their performance for 10 minutes, while each relay sends transactions with an increasing rate. Fig. 5 shows the achievable transaction throughput and latency as averaged for the elapsed 10 minutes and for the two sidechains as the request rate of each relay increases. As relays generate more messages per second, the Leader attempts to publish an increasing amount of blocks, creating extra network traffic due to the consensus protocol's voting mechanism. This saturates the throughput and increases latency for more demanding data exchange. However, this cost is countered by the inherent security characteristic that the blockchain architecture introduces to the protection system.

Next, we fix the transaction generation rate of each relay at 20 tx/sec and examine how the sidechain size impacts the system's performance. Fig. 6 shows the average throughput